Magistrate Judge Brian A. Tsuchida

09-MJ-00079-CMP

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

FREDERICK EUGENE WOOD,

Defendant.

CASE NO. MJ09-79

COMPLAINT for VIOLATION

Title 18, U.S.C.
Sections 1028A, 1030(a)(4), and 1343

BEFORE Brian A. Tsuchida, United States Magistrate Judge, U. S. Courthouse, Seattle, Washington.

The undersigned complainant being duly sworn states:

COUNT ONE

(Wire Fraud)

A. Background

At all times material herein,

1. FREDERICK EUGENE WOOD was a resident of Seattle, in the Western District of Washington.

2. The computer servers hosting the Craigslist website were located in San Francisco, California, and Scottsdale, Arizona.

3. FREDERICK EUGENE WOOD devised and effected a wire fraud scheme, described below, which included the use of Limewire, a "peer-to-peer"

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

computer "file sharing" program.

4. Peer-to-peer computer programs enable their users to create decentralized, peer-to-peer ("P2P") networks of computers. P2P networks provide a ready-made infrastructure for electronic file sharing by which files stored electronically on any computer that is part of the network can be "published" or "shared" with any other computer that is a member of the network, regardless of the physical location of the respective computers.

5. P2P networks and file sharing programs can be used legitimately for authorized and legal file sharing. P2P networks are, however, also known for, and commonly used to facilitate the unauthorized and illegal replication of copyright-protected music and videos files, among network members.

6. For individuals who are using a P2P network and program to share and replicate music and video files, it is beneficial to run the program constantly, and to configure any computer security protection firewalls to treat the P2P program as a "trusted" program. This configuration negates the protection normally afforded by firewall and anti-virus programs.

7. Limewire is a P2P file sharing program that can be downloaded, for free, from a website on the Internet at www.limewire.com. The Limewire program's default settings enable it to run constantly, and thereby to allow users constantly to share files. The Limewire program also automatically configures firewall programs to view Limewire as a trusted program, thereby negating the protection afforded by firewall and anti-virus programs.

8. A number of P2P programs exist, and a number of different versions of each program can exist. Some versions of some P2P programs have, by default, made a user's entire computer hard drive accessible to other members of the P2P network. Other versions of P2P programs, including the most recent version of Limewire, allow a user to create a folder on the user's computer's hard drive entitled, "shared," in which the user can place files he/she wishes to share. If the user is inexperienced or

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

not attentive, however, any file stored on the computer can be mistakenly included in the "shared" folder. Computer "viruses" also exist which can effectively expand access by a P2P network member to data beyond that stored in the designated "shared" folder.

A. The Offense

9. Beginning at a date uncertain, but in or about July, 2007 and continuing until on or about July 31, 2008, within the Western District of Washington and elsewhere, FREDERICK EUGENE WOOD did knowingly and willfully devise and intend to devise a scheme and artifice to defraud, and for obtaining money and property by means of material false and fraudulent pretenses, representations, and promises; and in executing and attempting to execute this scheme and artifice, did knowingly cause to be transmitted in interstate commerce by means of wire communication certain signs, signals, and sounds.

B. Essence of the Scheme and Artifice to Defraud

10. The essence of the scheme and artifice to defraud was that FREDERICK EUGENE WOOD would use the P2P file sharing networks afforded by Limewire to surreptitiously and illicitly steal identity (including social security number), and also banking, financial and tax return information that had been stored by others on their computers; that FREDERICK EUGENE WOOD would then use the identity and also banking, financial and tax return information that belonged to others, without their knowledge or consent, to produce counterfeit checks and also counterfeit driver's licenses in the names of others, or to open, or attempt to open online credit accounts or secure loans under the names of others; that FREDERICK EUGENE WOOD and others would use the counterfeit checks in conjunction with the counterfeit driver's licenses FREDERICK EUGENE WOOD had produced to fraudulently purchase merchandise, including computers, or would incur charges on fraudulently opened credit accounts; that FREDERICK EUGENE WOOD would use a computer and the Internet to "post" advertisements for the sale of fraudulently purchased computers on

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

the "Craigslist" Internet website; that FREDERICK EUGENE WOOD would then sell the fraudulently purchased computers to others, at a substantial discount, or, in some cases, would purport to sell a computer that he had advertised for sale on Craigslist, but would instead sell the would-be buyer a computer box containing something other than a computer; and that once FREDERICK EUGENE WOOD had accepted funds for the sale of these computers or computer boxes, he would convert the proceeds thereof to his own personal use and benefit.

C. **The Scheme and Artifice to Defraud**

11. It was part of the scheme and artifice to defraud that FREDERICK EUGENE WOOD knew that P2P programs, such as Limewire, are present on many family and home computers, located across the nation and the world, and that the P2P programs often are installed on those computers either by children, without the knowledge or permission of their parents, or by adults who are themselves also unaware that Limewire can make data and files stored on their computers accessible to strangers who are part of the Limewire network.

12. It was further part of the scheme and artifice to defraud that FREDERICK EUGENE WOOD knew that, with the use of his own computer and the Limewire P2P network, he could under some circumstances access a wide range of information, documents and data stored electronically on other computers hosting the Limewire program, including social security numbers, bank statements and federal income tax returns that had been stored electronically by other real people on and in their own private computers. FREDERICK EUGENE WOOD knew that he could access information on these computers regardless of their geographic location.

13. It was part of the scheme and artifice to defraud that FREDERICK EUGENE WOOD utilized a computer in Seattle, Washington, containing P2P software in order to facilitate and further his fraud scheme, with the result that his computer would become part of an interstate P2P file sharing network that provided him with direct peer-to-peer access, over the Internet, to other computers, on which the program

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

had been installed, regardless of their geographic location.

14. It was further part of the scheme and artifice to defraud that FREDERICK EUGENE WOOD intended to, and successfully did, by means of interstate P2P networks, surreptitiously gain access to identity and also banking, financial, and tax return information of other, real people that had been stored electronically on their private computers, without their knowledge, authorization, or consent, and that the computers to which FREDERICK EUGENE WOOD thereby gained access were located in many states, including Massachusetts, New York, Georgia, Florida, Ohio, Iowa, Louisiana, Oregon and California.

15. It was further part of the scheme and artifice to defraud that FREDERICK EUGENE WOOD did, through the use of the Limewire program, specifically "search" within the computers of others for bank and financial statements, account information, and federal income tax returns that had been stored electronically by other real people on and in their own private computers.

16. It was further part of the scheme and artifice to defraud that FREDERICK EUGENE WOOD would and did in turn use the identity, and also banking, financial, and tax return information that he surreptitiously and illicitly obtained from the electronically stored files on computers of other people to produce counterfeit checks and driver's licenses containing identity and bank account numbers of other real people. FREDERICK EUGENE WOOD used his computer to produce both the counterfeit checks and the counterfeit driver's licenses.

17. It was further part of the scheme and artifice to defraud that FREDERICK EUGENE WOOD would use the identity (including social security number information), and also banking and financial information that he surreptitiously and illicitly obtained from the electronically stored files on computers of other people to open or attempt to open credit accounts "online," over the Internet, in the names of the other real people whose identities he had stolen.

18. It was further part of the scheme and artifice to defraud that FREDERICK

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

EUGENE WOOD and others would use the counterfeit checks, together with the counterfeit driver's licenses that FREDERICK EUGENE WOOD had produced, to purchase merchandise, including computers.

19. It was further part of the scheme and artifice to defraud that FREDERICK EUGENE WOOD would use a computer and the Internet to "post" advertisements for the sale of fraudulently purchased computers on the "Craigslist" Internet website.

20. It was further part of the scheme and artifice to defraud that once FREDERICK EUGENE WOOD had arranged, via Craigslist and then through subsequent e-mail communications for a sale of fraudulently purchased merchandise, he would instruct the would-be buyer to meet him at a location in the Seatttle, Washington, area.

21. It was further part of the scheme and artifice to defraud that, in some instances in which he had arranged to sell a computer to a would-be buyer, FREDERICK EUGENE WOOD would accept the agreed upon funds for the sale from the would-be buyer, but in return for those funds, FREDERICK EUGENE WOOD would give the would-be buyer a sealed computer box, that contained a book and/or other objects, instead of a computer.

D. Execution of the Scheme and Artifice to Defraud

22. On or about November 14, 2007, within the Western District of Washington and elsewhere, for the purpose of executing and attempting to execute this scheme and artifice to defraud, FREDERICK EUGENE WOOD knowingly caused to be transmitted in interstate commerce by means of wire communication, certain signs, signals, and sounds, that is, an electronic posting over the Internet to the Craigslist website of an advertisement for the sale of a MacBook Pro 15.4" Matte computer, 2.2 GHz 2.0 GB RAM, for a price of $1500.00, which computer FREDERICK EUGENE WOOD thereafter agreed, via e-mail communications, to sell to D.M., of Seattle, Washington, for $1500.00, and for which sale FREDERICK EUGENE WOOD took and received $1500.00 from D.M. on November 15, 2007, but

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

in exchange for which funds FREDERICK EUGENE WOOD provided to D.M. a computer box, containing only a book and a glass vase, instead of a computer.

All in violation of Title 18, United States Code, Section 1343.

COUNT 2

(Accessing Protected Computer without Authorization to Further Fraud)

1. Paragraphs 1 through 22 of Count 1 are realleged and incorporated as if fully set forth herein.

2. On or about October 31, 2007, through on or about November 25, 2007, within the Western District of Washington and elsewhere, FREDERICK EUGENE WOOD knowingly and with intent to defraud, accessed protected computers without authorization and in excess of authorization, and by means of such conduct furthered an intended fraud by obtaining identity and banking information that belonged to R.M., of Staten Island, NY, and identity and banking information that belonged to C.C., of Warren, OH, which information FREDERICK EUGENE WOOD then used fraudulently to counterfeit checks, and which counterfeit checks FREDERICK EUGENE WOOD and others then used, in turn, fraudulently to purchase merchandise exceeding $5,000 in value within a period of one year.

All in violation of Title 18, United States Code, Section 1030(a)(4) and (c)(3)(A).

COUNT 3

(Aggravated Identity Theft)

1. Paragraphs 1 through 22 of Count 1 are realleged and incorporated as if fully set forth herein.

2. On or about October 31, 2007, within the Western District of Washington and elsewhere, FREDERICK EUGENE WOOD knowingly transferred, possessed and used, without lawful authority, a means of identification of another person, to wit, the

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

personally identifiable bank account number of R.M., of Staten Island, NY, during and in relation to a felony listed in Title 18, United States Code, Section 1028A(c), to wit, Fraud and Related Activity in connection with Computers, in violation of Title 18, United States Code, Section 1030(a)(4).

All in violation of Title 18, United States Code, Section 1028A(a)(1).

And the complainant states that this Complaint is based on the following information:

I, ROBERT D. RODRIGUEZ, being first duly sworn on oath, depose and say:

1. I am a Special Agent ("SA") of the Social Security Administration, Office of Inspector General, Office of Investigations ("SSA-OIG"), and have been so employed since May, 2006. I am currently assigned to the SSA-OIG field office in Seattle, Washington.

2. As an SA with SSA-OIG, my duties include the investigation of federal criminal offenses, particularly those involving Social Security fraud and identity theft. Social Security fraud includes the theft and fraudulent use of Social Security numbers. I have learned in the course of my work as an SA with SSA-OIG, and through my interactions with other federal law enforcement agents, that Social Security numbers are commonly stolen and used fraudulently in the context of other fraud schemes, including bank fraud, wire fraud, and mail fraud schemes. Through my work and collaboration with other federal law enforcement agents, I have become familiar with a variety of fraud schemes involving the use of fraudulent Social Security numbers and counterfeit identification documents.

3. I hold a Bachelor of Arts Degree in Criminal Justice from Seattle University. I have successfully completed both the twelve week criminal investigator training program and the four week inspector general investigative training program at the Federal Law Enforcement Training Center. As part of my training, I have received instruction on a wide range of federal criminal activities including theft from federally

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

funded programs, identity theft, Social Security fraud, and other financial crimes. I have also received training regarding the application for, and execution of federal arrest and search warrants.

3. The information contained in this affidavit is based on my own investigation, as well as the investigations of other law enforcement officers. Because this affidavit is submitted for the limited purpose of establishing probable cause for a criminal complaint, it does not contain and I have not here set forth herein all that I know about this case.

4. This affidavit is made in support of a complaint for the arrest of FREDERICK EUGENE WOOD for violations of Title 18 USC §§ 1028(A) (Aggravated Identity Theft), 1030(a)(4) (Fraud and Related Activity in Connection with Computers), and 1343 (Wire Fraud). I believe FREDERICK EUGENE WOOD is the defendant's true identity. FREDERICK EUGENE WOOD is a white male, light brown hair, hazel eyes, and approximately six (6) feet four (4) inches tall, 190 pounds.

5. The federal criminal investigation of FREDERICK EUGENE WOOD began after Detective Stacy Litsjo of the Seattle Police Department ("SPD") Fraud and Forgery Unit sought assistance with the SPD investigation into FREDERICK EUGENE WOOD and his possible computer related crimes, including identity theft. Detective Litsjo suspected FREDERICK EUGENE WOOD of using a "peer-to-peer," "file sharing" computer program called "Limewire" to steal personal identification information from victims.

6. Based on my training and experience, I know that Limewire, like other file sharing programs such as "Kazaa" and "Napster," is known, and commonly used for its ability to facilitate the unauthorized replication of copyright-protected music and video files. Limewire can be downloaded, for free, from a website on the internet at www.limewire.com. Once installed on a computer, the Limewire program allows "peer-to-peer" access. In other words, Limewire allows private individuals to access the computers of other individuals who also have installed the program on their computer in

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

order to share files like music, photographs, and videos.

7. After my assignment to the FREDERICK EUGENE WOOD investigation, I reviewed SPD incident report numbers 2007-464757, and 2007-471371. These reports detailed a reportedly fraudulent sale of an Apple Macintosh Pro laptop computer, and, in its aftermath, the related arrest of FREDERICK EUGENE WOOD. Based on these two reports, I learned the following:

8. On the 14th of November, 2007, the complaining victim ("D.M.") had seen an advertisement on the "Craigslist" website for the sale of a "brand new" Apple MacBook Pro computer. D.M. had made contact with the person advertising the computer via Craigslist and also e-mail, and thereby made arrangements to meet him at a Seattle location in order to purchase the computer. The seller had identified himself as "Ken." On November 15, 2007, D.M. met up with "Ken" and, after asking him some questions to verify that the computer was as advertised on Craigslist, D.M. paid Ken $1,500, and Ken turned over to D.M. what he believed to be an Apple MacBook Pro computer in its original sealed box. Once D.M. arrived home and opened the computer box, however, he found that it instead contained a book and a glass vase.

9. D.M. then recontacted Ken via e-mail, but this time with a different online user name. Ken said he no longer had the MacBook Pro for sale, but could sell D.M. a Mac Book computer. D.M. and Ken negotiated a price for this computer, and D.M. again arranged to meet with Ken to buy this second computer. In the meantime, D.M. had also advised SPD of this proposed meeting. SPD officers made a decision to be present at the meeting site, and that one of them would pose as the would-be buyer.

10. On November 20, 2007, D.M. and the SPD officers appeared at the designated location in Seattle. The person that D.M. knew as "Ken," and who had "sold" D.M. the computer box on November 15, also appeared in the same vehicle he had driven the week before. D.M. positively identified Ken to the SPD, and the SPD arrested Ken. "Ken" was booked into King County Jail and positively identified as FREDERICK EUGENE WOOD.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

11. Officers located an Apple computer box on the front passenger seat of WOOD's vehicle. When officers opened it, they found a book inside. Officers also found a wallet in the center console of the vehicle, that contained eight different and apparently counterfeit Washington State driver's licenses. The licenses all had FREDERICK EUGENE WOOD'S picture on them, but contained different names, addresses, and birthdates. The names on the cards were, "James Jude Kettinger Jr.," "David Martin Brubakken," "Thomas F. Kaczmaryc, Jr.," "Thomas William Faustner," and "Frederick E. Wood Jr." Officers also found an Apple Macintosh Pro Computer (serial number W87418SMX91) in WOOD's vehicle, which they placed into evidence.

12. As part of my investigation I learned from Detective Litsjo that she knew FREDERICK EUGENE WOOD to be an associate of Gregory Thomas Kopiloff. I know from Federal District Court records that Gregory Thomas Kopiloff was recently convicted in the Western District of Washington for Mail Fraud, Unauthorized Access to a Computer to Further Fraud, and Aggravated Identity Theft, in connection with a scheme to defraud over 80 individuals through the use of Limewire, a "peer-to-peer," "file sharing" software program that he used to access victims' computers and and steal their identity and financial information (CR07-0309). According to Detective Litsjo, she believed FREDERICK EUGENE WOOD taught Gregory Thomas Kopiloff how to use Limewire to commit fraud.

13. As part of her investigation, Det. Litsjo applied for, and obtained a search warrant for the Apple Macintosh Pro Computer (serial number W87418SMX91) that was present in FREDERICK EUGENE WOOD's vehicle. SPD Detective Dave Dunn (who is also a member of the U.S. Secret Service Electronic Crimes Unit and a certified computer forensics examiner), thereafter conducted a forensic examination of the data imaged from that computer. Det. Dunn completed a report of his investigation, which I have reviewed.

14. Det. Dunn's report of his forensic exam of WOOD's Apple Macintosh Pro Computer included the following information: WOOD's computer contained files containing hundreds of financial and other personally identifiable documents belonging to

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

other people. The documents included bank statements, copies of tax returns, at least one social security card and one birth certificate, loan documents, and other personal and financial documents. Based on electronic evidence contained in the computer, Det. Dunn was also able to determine that the documents had been obtained through the use of Limewire peer-to-peer file sharing software.

15. As part of this investigation, I attended a meeting at the Seattle FBI Office in August 2008, at which detectives and agents from SPD and the King County Sheriff's Office, and several federal law enforcement agencies met to discuss the results of the Det. Dunn's computer forensic examination, and the investigation. Detectives and agents subsequently catalogued the personally identifiable information found in the documents stored on WOOD's computer, from which they identified approximately 120 victims. Inspector Joe Stephenson of the U.S. Postal Inspection Service sent out survey letters to those identifiable victims. Approximately three dozen responses were received, with these respondents uniformly indicating that they did have computers connected to the Internet, and had not given any one permission to have the document of theirs that had been found on WOOD's computer. Many of the respondents acknowledged that Limewire had been on their computers, although many also indicated that they had not previously been aware of its presence on their computers. A total of 14 respondents reported that their personal identity information, Social Security number, or financial information had been used recently in a fraudulent way. In some instances, it had been made a part of counterfeit checks, in other cases, they had learned that the social security number and/or other identifying information had been used to open, or attempt to open unauthorized credit accounts in their names.

16. The documents found on WOOD'S computer included bank account statements of R.M., a resident of Staten Island, New York. The documents of R.M. found on WOOD'S computer were titled:

"JPMCStatement-.pdf"; "StatementRequest-3.pdf"; "StatementRequest-6.pdf"; "StatementRequest-7.pdf"; "StatementRequest-15.pdf"; and "StatementRequest-16.pdf."

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

These documents appeared to be statements of R.M.'s Chase Bank account, and included the full bank account number.

17. R.M. responded to the USPIS Postal survey, reporting that three (3) counterfeit checks had been written using the information of his Chase bank account. R.M. enclosed copies of the three (3) counterfeit checks. I have reviewed those copies of the counterfeit checks and observed that all three (3) checks purport to be drawn on an account with Bank of America, two (2) checks in the name of "J Jude Kettinger Jr." and the third in the name of "Jacob J. Kettinger Jr." However, upon closer inspection of the numerical information at the bottom of the checks, it contains a Chase bank routing number and R.M.'s Chase bank account number.

18. Based upon my investigation of this case, I recognized the name, "J Jude Kettinger Jr." on two (2) of the checks as almost identical to the name "James Jude Kettinger Jr." found on one of the fraudulent driver's licenses in FREDERICK EUGENE WOOD'S vehicle. The third check also had a similar name of "Jacob J. Kettinger Jr." Upon further review, I observed the third check was written to "CompUSA" on October 31, 2007 for $2,549.96.

19. On October 6, 2008, I contacted the corporate headquarters for CompUSA. I provided them with the date of the transaction, along with the amount, and payment method. Using this information they were able to locate the specific transaction and provided me a duplicate copy of the sales receipt and computer registration information. The sales receipt shows the purchase of an Apple Macintosh Pro computer, along with three additional items for a total of $2,549.96 from the CompUSA store in Jantzen Beach, OR on 10/31/2007, by a person named "Jacob Kettinger." The receipt also shows the serial number of the computer purchased as "SW87418SMX91." I checked the Seattle Police Department incident report regarding the computer found in FREDERICK EUGENE WOOD'S vehicle and confirmed it had the same serial number as the computer purchased from Comp USA using the fraudulent check drawn on the account of R.M.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

20. On February 12, 2009, Det. Dunn, in coordination with the U.S. Secret Service's Electronic Crimes Unit of New York, conducted a consensual forensic examination of R.M.'s computer. In his report of examination, Det. Dunn detailed how his examination did not locate the Limewire software as being currently installed on the computer, nor did he find the documents listed above that were found on FREDERICK EUGENE WOOD'S computer. However, he was able to locate multiple files that indicated Limewire had been installed on the computer at some point in the past, and had since been deleted. Detective Dunn was also able to locate remnants of the files found on FREDERICK EUGENE WOOD'S computer. These remnants indicated that these files had previously been on R.M.'s computer in a folder labeled "Grandpa Stuff."

21. On February 6, 2009, SA Joe Velling, SSA-OIG, and Det. Dunn interviewed FREDERICK EUGENE WOOD about the fraud conduct which is the subject of this investigation. After being advised of his rights, FREDERICK EUGENE WOOD admitted to using his computer, along with the Limewire program, to search for and obtain copies of people's personal financial documents. WOOD said he would use these financial documents to create counterfeit checks with the victim's personal financial information, manufacture a counterfeit identification to correspond with the counterfeit check, and then either by himself or with an associate, cash the check for goods at local stores.

22. FREDERICK EUGENE WOOD said that he would specifically use Limewire to search for documents with keywords, "statement," "account," and "tax.pdf." WOOD said that through Limewire, he was sometimes able to both download a file from someone's computer and also navigate to their share folder on their computer. He would sometimes do this and explore the local computer folder on the victim's computer. In response to Det. Dunn's question as to whether he thought people would willingly share this kind of information on the Internet, FREDERICK EUGENE WOOD responded that people don't understand how the software works, and that often times "kids put Limewire

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

on the computer and the parents don't know." He said that, by default, Limewire shared a lot of information from your computer.

23. FREDERICK EUGENE WOOD explained that after he had accessed and successfully obtained these types of documents from the computers of others, via Limewire, he would use information taken from those documents (such as bank account numbers), to produce counterfeit checks. He produced the counterfeit checks on his computer, with a check printing software. He would then use Adobe Photoshop to manipulate an ID template provided to him by Greg Kopiloff. WOOD said he would simply change the name and information on the IDs to match the check. WOOD stated that he had been storing some of his ID templates on a virtual drive, named "uderwearandmore@mac.com" or "underwearandmore@me.com."

24. FREDERICK EUGENE WOOD said that he had passed counterfeit checks using information he obtained from Limewire "30 - 40" times, and that on many of those occasions he had done so with an associate. SA Velling showed WOOD a copy of the counterfeit check bearing the financial information of R.M, but the name "Jacob Kettinger," that was used to purchase the Apple Macintosh Pro computer that was seized from him by SPD on the day of his arrest. WOOD identified the handwriting on the check as that of his associate, and said the associate was the one who actually purchased the computer from the store. WOOD said he was the one who printed the check, however, and also that he would have produced the counterfeit driver's license for that associate in order to help him pass the counterfeit check. WOOD stated that he had purchased 10-15 computers, which he then sold on Craigslist for 30% - 50% of their retail value. He would sometimes give the would-be customer an empty computer box, as he did when he was arrested by SPD.

25. When asked by SA Velling if he knew what he was doing was wrong and that the accounts he was using belonged to real people, FREDERICK EUGENE WOOD stated that, "[y]es, you have to be human."

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

26. Based on the forgoing, I submit that there is a probable cause to believe that FREDERICK EUGENE WOOD has committed violations of Title 18, United States Code, Sections 1028(A), 1030(a)(4), and 1343.

Robert Rodriguez

SA ROBERT RODRIGUEZ, Complainant
Social Security Administration, SSA-OIG,
Seattle, Washington

Based on the Complaint and Affidavit sworn to before me, and subscribed in my presence, the Court hereby finds that there is probable cause to believe the Defendant FREDERICK EUGENE WOOD committed the offenses set forth in the Complaint.

Dated this 2nd day of March, 2009.

BRIAN A. TSUCHIDA
United States Magistrate Judge

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970